Research of Social Engineering Attacks in Telecommunications Fraud

Guangxuan CHEN, GuominZHOU, Zhoujie MAO, Qiang LIU & Ziwan ZHENG
Zhejiang Police College, Hangzhou, China

Guangxiao CHEN
Shanghai Industry and Commerce Foreign Language College, Shanghai, China

Panke QIN
College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, China

ABSTRACT: Telecommunications fraud is spreading rapidly in some areas of China, which caused huge losses to the people's property. This paper analyzed the weakness and psychological factors of the victims, and revealed the nature of telecom fraud, i.e., the criminal’s skilled use of social engineering for fraud, harm, and other dangerous acts, so as to obtain their own interests. In order to better combat and prevent telecom fraud, countermeasures from all angles are given. The government and law enforcement need to put more effort in the anti telecom fraud campaign and propaganda work and education programs must promptly follow up. And ordinary people need to overcome their own weakness as timid, greedy, curiosity, blind trust, and develop safety awareness, enhance privacy protection.
KEYWORD: Telecommunications fraud; Social engineering; Human weakness; Psychological factors

1 INTRODUCTION

With the fast development of the financial, telecommunications, Internet and other modern industries, telecommunications fraud through network facilities and telecommunication infrastructure is spreading rapidly in some areas of China. Aiming to specific populations, the telecom fraudsters impersonate staff of bank, police, taxation, social security, telecommunication and other relative department, set up scams and con schemes of all kinds, fabricate false information, entice even intimidate the victim through telephone, VoIP phone, SMS or online chat, so as to let the victims transfer the money to the account they established. Once the transfer is completed, the criminals will draw the money in the account in the shortest time, thus the last link of the entire telecom fraud is completed. Throughout the whole process of the fraud, the victims are always manipulated remotely and have known nothing about the fraudsters even when they found they were fraud.

In these emerging telecom frauds, the criminal means and techniques are multifarious, causing a great loss to people’s property. Throughout the world, telecom fraud has been existed in various forms for decades. According to the estimation of US CFCA (Communications Fraud Association), the loss resulting from telecom fraud each year is more than 60 billion US dollars. And in China, the statistics showed that in 2008, victims in Fujian, Guangdong, Shanghai and Beijing have been fraud as many as more than 600 million yuan; in the first quarter of 2009, people in Beijing have been cheated more than 68 million yuan and Guangdong more than 80 million yuan (Hu & Liu 2010); in 2011-2014, the amount of money involved in the telecom fraud in economically developed areas of the country have reached a billion yuan every year, and there is an upward trend. According to the data from Ministry of Public Security, there are more than 300,000 cases of telecom frauds and more than 10 billion yuan involved in China. The severe situation of telecom fraud in recent years in China is shown in Figure 1. Recently, the criminals have expanded their target from the coastal areas throughout the country. As can be learn from the public security bureau, telecom fraud occurred frequently in some economically undeveloped remote areas these days.

The law enforcement of China has paid great attention to the telecom fraud and always insists on fighting the criminals. They have token a series of special operations on the issues and achieved many achievements. However, there are still many careless people have been deceived. The reasons of this passive situation are various, in addition to technique difficulties (for example, the criminals adopted a series of advanced technologies, such as VoIP technology, bulk SMS technology, phone number changing technology, and so on) and jurisdiction and cooperation difficulties (telecom fraud is often cross-regional and cross-border and the members of the

criminal group are often located in different regions or countries to jointly implement the crime), the social engineering hidden in the telecom fraud is the key factor that made people gullible and vulnerable to fraudsters. The criminals take advantage of ordinary people's weakness and set up various traps to lure or threat the victims. It can be said, the telecom fraudsters are social engineering masters that make them successfully commit the crime and easily get away from the punishment.

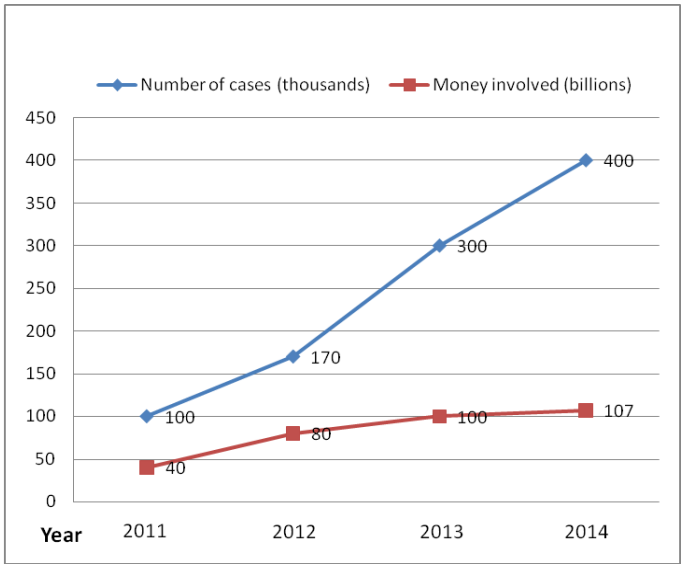

Figure 1. The severe situation of telecom frauds in recent years in China

2 SOCIAL ENGINEERING

2.1 *Definition of social engineering*

Social engineering (SE) is an emerging science that uses human error or weakness (i.e. 'cognitive biases', such as curiosity, greed, fear and forgetfulness) to gain useful information or access to any system (Mitnick & Simon 2004, Gold 2010). It plays on the trust element of the human nature and usually involves psychological and technical aspects in order to gain the victim's trust. SE is originally a concept in information security field that proposed by the former US number one hacker Kevin Mitnick in his book "The Art of Deception" which aims to education people to be vigilant and avoid being cheated.

2.2 *Social engineering attack in information security field*

As the telecommunications industry, financial industry and internet industry continue to improve the securities, the direct use of technical weakness of the system or organization to carry out crime has become increasingly difficult. So, the criminals are turning to the manipulation of human error and human weakness. They can achieve their goals through social engineering attack with lower cost. As Kevin Mitnick once said: "human are the weakest link in the security system. We can be equipped with the best defense technology and most advanced facilities, such as firewall, IDS, vital statistics equipments, however, a master of social engineering can get whatever he need by making a phone to a man without any protective mind."

In the tradition information security field, the development of security and defense usually focused on improving the material and technology factors (such as the latest technology and equipment) and external behavioral factors (such as service, management, etc.), while ignored the core factor in the security system, i.e. human factor. Therefore, the well constructed security defense system usually become vulnerable when faced with social engineering attack, which can bypass the most solid line of defense and directly attack the human weakness, the weakest link of the system. Report of information security and risk study from the Gartner claimed that the social engineering will be the biggest security risks in the next decades. In addition to the various ways in the information security field, such as steal information, invasion and destruction, phishing and Trojans, social engineering has played a great role in telecom fraud, which caused huge losses to the people's property.

3 SOCIAL ENGINEERING BEHIND THE TELECOM FRAUD

The ways of telecom fraud are various, where the most common four types are fixed telephone fraud, mobile phone fraud, e-mail scam and internet phone scam (or VoIP scam). Table 1 showed the statistical data of these four types of telecom fraud occurred in Foshan City in Guangdong province in 2010-2012 (Huang 2013).

In addition to the help of advanced technology, equipment and tools, the key factor in the telecom fraud is social engineering attack. The criminals collect the information of the potential victims, carpet sending fraudulent messages to the potential victims or make massive calls to the victims, and then launch social engineering attack to the fooled victims so as to achieve their hidden goals. The common work flow of social engineering attack behind telecom fraud is shown in Figure 2.

Through the analysis of a large number of cases occurred in recent years, we found that the typical telecom fraud using social engineering attack can be summed into following types, in which the criminals fully grabbed the victim's psychology and took advantage of their weakness.

Table 1. The most common four types of telecom frauds in the surveyed city Foshan (unit of lost: yuan)

	Year	2010	2011	2012
Fixed telephone fraud	Number of cases	87	93	78
	Total lost	204450	145080	67080
	Average lost	2350	1560	860
Mobile phone fraud	Number of cases	275	332	486
	Total lost	2432375	1153700	1044900
	Average lost	8845	3475	2150
E-mail scam	Number of cases	52	32	37
	Total lost	7976800	3847010	3543860
	Average lost	153400	12020	95780
Internet phone scam	Number of cases	886	1013	1324
	Total lost	8507758	5541110	3186863
	Average lost	9600	5470	2406

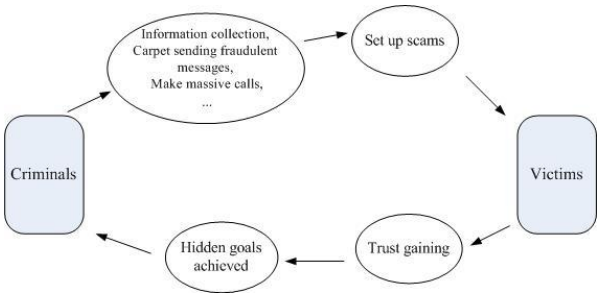

Figure 2. Common work flow of social engineering attack behind telecom frauds

3.1 *Timid, fear and superstitious about "authority"*

Timid and afraid of "authority" are the reflections of some people with low psychology quality. They believe without a shadow of doubt in the authorities' claims. These "authorities" can be public security bureau, court, bank, telecom bureau, hospital, or leaders, superiors, even the kidnappers. The criminals can grab the victim's psychology through the dialogue within minutes and impersonate as people from the authorities to set up various scams. The victims were commonly told that they have involved in cases as money laundering, drug trafficking or buying of sex, and asked to cooperate with the investigation and need to transfer the money to an authority account as bail. People with weak psychology bearing capacity are likely to be deceived.

3.2 *Greedy*

Greed is one the human nature and a fatal weakness and is frequently used by social engineering attacker in the information security field. It's disturbing that the use of victim's greed is extended into telecom frauds, such as the fraudsters set up scams as winning the lottery, cheap flights, unsecured loans, false tax refund of houses (or cars, education, goods, etc), false stock information, false matchmaking, and so on. Usually, the criminals will promise to the victims some benefit by sending short message or calls so as to lure victims to the bait they set up.

3.3 *Curiosity*

Curiosity is a quality related to inquisitive thinking such as exploration, investigation, and learning, evident by observation in human and many animal species (Berlyne 1954). In the psychology field, curiosity refers to the psychological inclinations as awareness, operation and asking that brought from the people when they encounter something new or experience a new external environment. Different individuals have different degrees of curiosities. Curiosity is one of the intrinsic motivations of learning of the individual, but also an important feature of creative talents. However, excessive curiosity will bring adverse affect to the individual. Social engineer often takes advantage of victim's curiosity to carry out attacks, such as they often put some hot issues, belle images, celebrity privacy or "insider information" to lure the recipients to open the attachments, so as to intrude and control the victim's computer.

From a larger number of telecom fraud cases we know, the criminals often take advantages of victim's curiosity to carry out fraudulent activities, such as they frequently send massive SMS about fictitious information of firearms and ammunition, eavesdropping equipment, micro videotaping equipment, ecstasy and other forbidden objects, so as to lure the curious victims to pay them deposit, haulage, security fee.

4 PREVENTION STRATEGIES FOR SOCIAL ENGINEERING ATTACKS

Due to the high-profile crackdowns, telecom fraudsters are changing their fraud methods constantly. The prevention and combat of telecom fraud and social engineering needs the joint effort from the government, ordinary people and social organizations.

As for the government and law enforcement, they should first put more power on fight the telecom fraud, such as strength cooperation between countries and regions, organize and guide different departments as public security bureau, Procuratorate, court, financial sections and telecommunication departments to cooperate with common effort. The registration department of public information and all

kinds of departments that involve personal information gathering should strengthen information security work, so as to reduce the opportunities for the criminals to obtain the personal information. In addition, security education is necessary. The government should frequently launch education activities for the people through all kinds of means.

As for the ordinary people, they should first overcome the human weakness as timid, fear and superstitious about "authority", greedy, curiosity, and so on. Make sure never disclose the personal information and family information on the internet or other places. Never believe the so called "case information" from the "public security bureau" or "Procuratorate". Never believe the calls about bank account updating information from the "bank staff". And be sure to remember that there is no such thing as a free lunch.

As for the social organizations, they should cooperate with the government for the publicity and education work, so as to enhance the people's awareness of the security. Such as, the community should frequently launch education activities to help the neighbors, especially the old people, to identify the newest telecom fraud methods.

Human are vulnerable, once they are manipulated or personal information has leaked out, unexpected consequence will appear in front of them. In order to prevent telecom fraud, we should first know well about it and understand how it works, and more importantly, we should see clearly the social engineering attacks hidden in it. Only we increase the safety awareness and develop rational thought, we will not become the lamb of "Art Deception".

5 CONCLUSIONS

This paper introduced the social engineering behind the telecom frauds in recent years. Social engineering is a science about how to explore human weakness to obtain self interests. Telecom fraudsters usually use social engineering techniques to swindle victims out of amounts of money. It's hardly to prevent the social engineering attacks through technical measures. In order to better combat telecom fraud, it's critical to grasp the nature of the crime and understand the principle of social engineering hidden behind them. People should overcome the weaknesses and improve safety awareness. Public security departments, telecommunication authority and financial sectors should work together to resist and combat the crime from different angles and build security prevention and control mechanisms.

ACKNOWLEDGMENTS

This study is supported by College-level Scientific Research Program of Zhejiang Police College (No. 20140629), Scientific Research Project of Zhejiang Educational Department (No.Y201329872), and Fund of Key Laboratory of Public Security Information Application Based on Big-data Architecture, Ministry of Public Security, P.R. China.

REFERENCES

[1] Berlyne, D.E. 1954. A theory of human curiosity. *Br J Psychol* 45(3): 80-91.
[2] Berlyne, D.E. 1955. The arousal and satiation of perceptual curiosity in the rat. *J Comp Pyhsiol Psychol* 48(4): 38-46.
[3] Hu, X.Y. & Liu, X.W. 2010. Research on Prevention and Control Countermeasures of Telecom Fraud Crime. *Journal of Chinese People's Public Security University (Social Science Edition)* 147(5): 90-98.
[4] Mitnick, K. D. & Simon, W. L. 2004. *The Art of Deception: Control the Human Element of Security*. Wiley Publishing, Inc.
[5] Gold, S. 2010. Social Engineering Today: Psychology, Strategies and Tricks. *Network Security* (11):11-14.
[6] Lee, D.H. & Kyong, H.C. 2007. Intelligence Report and the Analysis Against the Phishing Attack Which Uses a Social Engi-neering Technique. *Lecture Notes in Computer Science* (4076): 185-194.
[7] Mitnick, K. D. & Simon, W. L. 2005. The Art of Intrusion. Wiley Publishing, Inc.
[8] Huang, L. 2013. Telecommunications fraud on Crime Prevention and Control System As Foshan city in Guangdong Province for example. *Dissertation for the Degree of Master of South China University of Technology*. 22-23.